Chapter 11
Miscellaneous

Section 1: TEMPEST

TEMPEST Requirements. When compliance with TEMPEST standards is required for a contract, the GPM/PSO will issue specific guidance in accordance with current national directives that afford consideration to realistic, validated, local threats, cost effectiveness, and zoning.

Section 2. Government Technical Libraries

SAP information will not be sent to the National Defense Technical Information Center or the U.S. Department of Energy Office of Scientific and Technical Information.

Section 3. Independent Research and Development

11-300. General. ***The use of SAP information for a contractor Independent Research and Development (IR&D) effort will occur only with the specific written permission of the Contracting Officer. Procedures and requirements necessary for safeguarding SAP classified information when it is incorporated in a contractor's IR&D effort will be coordinated with the PSO.***

11-301. **Retention of SAP Classified Documents Generated Under IR&D Efforts. With** the permission of the Contracting Officer, the contractor may be allowed to retain the classified material generated in connection with a classified IR&D effort. The classified documents may be required to be sanitized. If necessary, the Government agency will provide the contractor assistance in sanitizing the material to a collateral ***or*** unclassified level (i.e., by reviewing and approving the material for release).

11-302. Review **of Classified IR&D Efforts.** ***IR&D operations and documentation that contain SAP classified information will be subject to review in the same manner as other SAP classified information in the possession of the contractor.***

Section 4. Operations Security

Special Access Programs may require unique Operations Security (OPSEC) plans, surveys, and activities to be conducted as a method to identify, define, and provide countermeasures to vulnerabilities. These requirements may be made part of the contractual provisions.

Section 5. Counterintelligence (CI) Support

11-500. Counterintelligence (CI) Support. Analysis of foreign intelligence threats and risks to Program information, material, personnel, and activities may be undertaken by the Government Agency. Resulting information that may have a bearing on the security of a SAP will be provided by the Government to the contractor when circumstances permit. Contractors may use CI support to enhance or assist security planning and safeguarding in pursuit of satisfying contractual obligations. Requests should be made to the PSO.

11-501. **Countermeasures.** Security countermeasures may be required for SAPS to protect critical information, assets, and activities. When OPSEC countermeasures are necessary, they will be made a part of the contract provisions and cost implementation may be subject to negotiation. Countermeasures may be active or passive techniques, measures, systems, or procedures implemented to prevent or reduce the timely effective collection and/or analysis of information which would reveal intentions or capabilities (e.g., traditional security program measures, electronic countermeasures, signature modification, operational and/or procedural changes, direct attack against and neutralization of threat agents and/or platforms, etc.).

Section 6. Decompartmentation, Disposition, and Technology Transfer

11-600. *Every scientific paper, journal article, book, briefing, etc., pertaining to a SAP and prepared by personnel currently or previously briefed on the SAP that is proposed for publication or presentation outside of the SAP will be reviewed by the PSO and a Program-briefed Public Affairs Officer (PAO) if available. Any release will be by the GPM.* Often SAP-unique "tools" such as models, software, technology, and facilities may be valuable to other SAPS. Some information, material, technology, or components may not be individuall y sensitive. If information or materials can be segregated and disassociated from the SAP aspects of the Program, decompartmentation and release of the information and/or materials may be approved to support U.S. Government activities. *The information and materials proposed for release will remain within the Program Security Channels until authorized for release.*

11-601. Procedures. The following procedures apply to the partial or full decompartmentation, transfer (either to another SAP or collateral Program), and disposition of any classified information, data, material(s), and hardware or software developed under a SAP contract or subcontract (SCI information will be handled within **SCI** channels).

a. **Deeompartmentation.** *Prior to decompartmenting any classified SAP information or other material(s) developed within the Program, the CPSO will obtain the written approval of the CPM. Decom - partmentation initiatives at a Program activity will include completion of a Decompartmentation or Transfer Review Format Include supporting documentation that will be submitted through the PSO to the GPM. Changes, conditions and stipulations directed by the GPM will be adhered to. Approval of Program decompartmentation and all subsequent transfers will be in writing.*

b. **Technology Transfer.** Technologies may be transferred through established and approved channels in cases where there would be a net benefit to the U.S. Government and Program information is not exposed or compromised. The Contracting Officer is the approval authority for technology transfers.

(1) Contractor Responsibilities. *CPSOs will ensure that technologies proposed for transfer receive a thorough security review. The review will include a written certification that all classified items and unclassified Program-sensitive information have been redacted from the material in accordance with sanitization procedures authorized by the GPM. A description of the sanitization method used and identification of the official who accomplished the redaction will accompany the information or* material(s) *forwarded to the GPM for review and approval*

(2) Government Responsibilities. The contracting officer's representative (COR), PSO, and GPM will make every attempt to review requests expeditiously. ***Requests will be submitted at least thirty (30) working days prior to the requested release date.*** This is particularly important when requesting approval for Program-briefed personnel to make non-Program related presentations at conferences, symposia, etc.

Section 7. Other Topics

11-700. Close-out of a SAP. *At the initiation of a contract close-out, termination or completion of the contract effort, the CPSO will consider actions for disposition of residual hardware, software, documentation, facilities, and personnel accesses. Security actions to close-out Program activities will prevent compromise of classified Program elements or other SAP security objectives. The* contractor may be required to submit a termination plan to the Government. The master classified material accountability record (log or register) normally will be transferred to the PSO at Program close-out.

11-701. Special Access Program Secure Communications Network. SAPS may use a SAP secure communications and/or data network linking the GPM and/or contractors with associated technical, operational, and logistic support activities for secure communications.

11- 702. Patents. *Patents involving SAP information will be forwarded to the GPM/PSO for submission to the Patents Office. The PSO will coordinate with Government attorneys and the Patent Office for submission of the patent.*

11-703. Telephone Security. The PSO will determine the controls, active or inactive, to be placed on telecommunication lines. *SAPFs accredited for discussion or electronic processing will comply with DCID 1/21 and Telephone Security Group (TSG) standards as determined by the PSO.*